UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF TEXAS
HOUSTON DIVISION

MILLENNIUM TGA, INC.	)	
Plaintiff,	)	CA. 4:11-cv-04501
v.	)	
JOHN DOE, and 938 UNNAMED CO-CONSPIRATORS	)	
Defendants.	)	

JOHN DOE 112'S CONSOLIDATED MOTION & MEMORANDUM TO QUASH SUBPOENA PURSUANT TO FED. R. CIV. P. 45

I. INTRODUCTION

Copyright infringement is a legitimate basis for suit, and if many people engage in copyright infringement, many people may be sued. However, the general safeguards developed by federal courts to ensure defendants get a fair chance to present their defenses always apply and, have a special importance in a case such as this.[1]

Plaintiff alleges that John Doe and his 938 'doe'-conspirators conspired to illegally reproduce and distribute Plaintiff's video "Shemale Yum—Jenna Comes A' Knocking!" ("the Work") using an Internet file sharing method known as BitTorrent. Complaint at ¶¶ 5, 25-38. In pursuit of its claims, Plaintiff filed for expedited discovery prior to a Rule 26(f) conference. Due to the *ex parte* nature of Plaintiff's motion, Plaintiff faced no opposition to fully expound on the prejudices that John Doe 112/IP Address 184.155.204.241 faces as a result.

Plaintiff's established business model is to use mass copyright litigation to extract settlements from individuals, regardless of guilt. To date, Plaintiff has filed no fewer than ten similar cases, none of which have adjudicated on the merits, in nine different jurisdictions against

[1] *See, e.g.*, U.S. Magistrate Judge Gary R. Brown's recent Order. *In re: Bittorennt Adult Film Copyright Infringement Cases*, 11-cv-03995-DRH-GRB, ECF No. 39 (E.D.N.Y Filed May 1, 2012).

a combined total of 3,807 defendants.[2] Despite changes in venue, Plaintiff's bad faith remains constant.

On December 7, 2012, Plaintiff filed a complaint in the District of Columbia captioned *Millennium TGA v. Does 1–939*, No. 1:11-cv-02176 (D.D.C. 2011) (hereinafter "*Millennium TGA I*"). Nine days later, Prenda Law, Inc. (Millennium TGA, Inc.'s attorneys) voluntarily dismissed the case once it was realized the judge assigned to their case, Judge Robert Wilkins, was antagonistic towards their pre-litigation tactics and goals. On December 20, 2012, four days after dismissing *Millennium TGA I,* Plaintiff re-filed essentially the same complaint here in the Southern District of Texas, as *Millennium TGA, Inc. v. John Doe*, 4:11-cv-4501-VG , (S.D. Tex. 2011) (hereinafter "*Millennium TGA II*"). ECF No. 1 ("Complaint"). Whereas *Millennium TGA I* named 939 Doe defendants, *Millennium TGA II* names one Doe defendant and alleged 938 Doe coconspirators. The 939 IP addresses identified in both actions are the same. (Compare *Millennium TGA I* Complaint at Ex. A (chart of Doe defendants) with *Millennium TGA II* Complaint at Ex. B (chart of Doe coconspirators).) So are Millennium's claims.

On February 29, 2012, Comcast objected to the subpoena in *Millennium TGA II,* stating that 1) the court lacked personal jurisdiction over most of the IP addresses listed in the subpoena; 2) there were serious joinder issues in the lawsuit; and 3) the plaintiff was engaging in "a blatant attempt to forum shop" since they already dismissed *Millennium TGA I* to avoid being in front of Judge Wilkins.

As a result, Prenda Law, Inc. filed a suit against Comcast. The action was actually a "motion to compel" in the Texas case (*Millennium TGA II)*, but was filed in the District of Columbia. *Millennium TGA, Inc. v. John Doe*, 1:12-mc-00150 (D.D.C. 2011) (hereinafter "*Millennium TGA III*"). On June 26, 2012, Judge Wilkins denied the motion to compel, in part,

---

[2] *Millenium TGA, Inc. v. Doe*, 12-cv-00792 (S.D. Cal. April 2, 2012); *Millenium TGA, Inc. v. Does 1-800*, 10-cv-05603 (N.D. Ill. Sept. 2, 2010); *Millennium TGA, Inc. v. Does 1-939*, 11-cv-02176 (D.D.C. Dec. 7, 2011); *Millennium TGA, Inc. v. Does 1-21*, 11-cv-02258, (N.D. Cal. May 6, 2011); *Millennium TGA, Inc. v. Does 1-60*, 12-cv-20938 (S.D. Fla. March 6, 2011); *Millennium TGA, Inc. v. Doe*, 11-cv-03080 (E.D. Cal. Nov. 21, 2011); *Millennium TGA, Inc. v. Does 1-939*, 11-cv-04501 (S.D. Tex. Dec. 20, 2011); *Millennium TGA, Inc. v. Doe*, 12-cv-01360 (E.D.N.Y. March 20, 2011); *Millennium TGA, Inc. v. Does 1-529*, 11-cv-032619 (11th Judicial Cir. for Miami-Dade County, Fla. 2011); *Millennium TGA, Inc. v. Does 1-515*, 11-cv-31922 (11th Judicial Cir. for Miami-Dade County, Fla. 2011).

because "the federal courts, and its subpoena power, are not to be used to gather information that is only relevant to invalid claims."[3]

In this particular context, the Court must balance "the need to provide the injured part[y] with an [sic] forum in which [it] may seek redress for grievances" against those of ISP subscribers "without fear that someone who wishes to harass or embarrass them can file a frivolous lawsuit and thereby gain the power of the court's order to discover their identity." *Columbia Ins. Co. v. Seescandy.com*, 185 F.R.D. 573, 578 (N.D. Cal. 1999). *See also, London-Sire Records, Inc. v. Doe 1*, 542 F. Supp. 2d 153, 163 & nn.10-11, 179 (D. Mass. 2008) (holding that the court must consider "the expectation of privacy held by the Doe defendants, as well as other innocent users who may be dragged into the case (for example, because they shared an IP address with an alleged infringer.").

> "Put another way, Article 1, section 8 of the Constitution authorizes Congress to enact copyright laws "to promote the Progress of Science and useful Arts." If all the concerns about these mass Doe lawsuits are true, it appears that the copyright laws are being used as part of a massive collection scheme and not to promote useful arts."

On the Cheap, LLC v. Does 1-5011, No. 10-cv-4472, 2011 U.S. Dist. LEXIS 99831, *12 n.6 (N.D. Cal. Sept. 6, 2011).

Plaintiff's established record of ill conduct indicates that it is now using this Court as nothing more than an inexpensive means to gain John Doe 112's personal information to coerce payment.

II. TECHNICAL BACKGROUND

A. Internet Protocol Addresses.

1. Definition.

Any subscriber of an Internet Service Provider ("ISP"), such as John Doe 112, who connects their computer to the Internet via the ISP is assigned an Internet Protocol (IP) address. *U.S. v. Heckenkamp*, 482 F.3d 1142, 1144 (9th Cir. 2007). In addition to the subscriber's IP address, the ISP's network is also assigned its own IP address. *LVRC Holdings v. Brekka*, 581 F.3d

[3] See Exhibit A - *Memorandum Opinion* for *Millennium TGA III.*

1127, 1130 (9th Cir. 2009). Typically, subscribers are assigned a dynamic IP address. That is, their ISP assigns a different IP address each time the subscriber logs on to their computer.[4]

2. Purpose.

The purpose of an IP address is to route traffic efficiently through the network. It does not identify the computer being used nor the user. IP addresses only "specify the locations of the source and destination nodes in the topology of the routing system."[5]

3. Identification.

To be clear, it is an account that is identified as being used to commit the infringing activity, *not* the subscriber of the account. Trying to use an IP address as a window through which the Plaintiff can see the identity of an actual infringer is futile. What Plaintiff sees instead is a router or wireless access point—not who did it. Nor is an IP address alone a reasonable basis to believe that a subscriber has infringed. A subscriber can be misidentified in multiple ways as an infringer without participating in any infringing behavior, including:

1. Some members of a swarm simply and automatically pass on routing information to other clients, and never possess even a bit of the movie file;[6]
2. A client requesting a download can substitute another IP address for its own to a Bittorrent tracker;[7]
3. A user can misreport its IP address when uploading a torrent file. A user in the network path between the user monitoring IP address traffic and the Bittorrent tracker can implicate another IP address;[8]
4. Malware on a computer can host and distribute copyrighted content without knowledge or consent;[9]

---

[4] ECF No. 2-1, ¶ ¶ 16-17 ("Hansmeier Declaration") ("A dynamic IP address is an IP address that will change from time-to-time." … "Most consumer customers of Internet service providers are assigned a dynamic IP address.")

[5] "IP Address" http://en.wikipedia.org/wiki/IP_address (Last visited May 9, 2012).

[6] Sengupta, S. et al., *Peer-to-Peer Streaming Capacity,* IEEE Transactions on Information Theory, Vol. 57, Issue 8, pp. 5072-5087, at 5073 (Prof. Helmut Bolcski, ed., 2011) ("A [BitTorrent] user may be the source, or a receiver, or a helper *that serves only as a relay.*") (emphasis added).

[7] Michael Piatek et al., *Challenges and Directions for Monitoring P2P File Sharing Networks—or—Why My Printer Received a DMCA Takedown Notice*, 3 (2008), http://dmca.cs.washington.edu/uwcse_dmca_tr.pdf *See also,* "IP address spoofing" http://en.wikipedia.org/wiki/IP_address_spoofing (Last visited May 9, 2012) (the term IP address "spoofing" refers to the creation of a forged IP address with the purpose of concealing the user's identity or impersonating another computing system.).

[8] Piatek at 4.

[9] *Id.*

5. There are reliability issues with using IP addresses and timestamps to identify the correct party;[10]

6. If a subscriber has dynamic IP addressing through its website host, it is sharing an IP address with several other subscribers;[11] or

7. Anyone with wireless capability can use a subscriber's wifi network to access the Internet, giving the impression that it is the subscriber who is infringing.[12]

For these reasons, many courts have recognized in similar cases that the ISP subscribers may not be the individuals who infringed upon Plaintiff's copyright.

> An IP address provides only the location at which one of any number of computer devices may be deployed, much like a telephone number can be used for any number of telephones. ... Thus, it is no more likely that the subscriber to an IP address carried out a particular computer function -- here the purported illegal downloading of a single pornographic film - than to say an individual who pays the telephone bill made a specific telephone call.
>
> Indeed, due to the increasingly popularity of wireless routers, it much less likely. While a decade ago, home wireless networks were nearly non-existent, 61% of US homes now have wireless access.... [A] single IP address usually supports multiple computer devices — which unlike traditional telephones can be operated simultaneously by different individuals… Different family members, or even visitors, could have performed the alleged downloads. Unless the wireless router has been appropriately secured (and in some cases, even if it has been secured), neighbors or passersby could access the Internet using the IP address assigned to a particular subscriber and download the plaintiff's film.

In re BitTorrent Adult Film Copyright Infringement Cases, Civ. A. No. 11-3995 (DRH) (GRB) 2012 U.S. Dist. LEXIS 61447, *8-9 (E.D.N.Y. May 1, 2012) (citations omitted). See also, *VPR Internationale* ***v.*** *Does 1-1017*, No. 11-cv-02068-HAB-DGB, 2011 U.S. Dist. LEXIS 64656, *3 (N.D. Ill. 2011). As a result, "the assumption that the person who pays for Internet access at a

---

[10] *Id.* ("When IP addresses are assigned dynamically, reassignment of an IP address from an infringing user to an innocent user can cause the behavior of the infringing user to be attributed to the innocent user. Because the monitoring client (copyright holder) records information from the tracker of the Bittorrent client, the information can quickly become inaccurate and will not implicate the correct user.")

[11] "Web hosting service" http://en.wikipedia.org/wiki/Web_hosting_service (Last visited May 9, 2012).

[12] Carolyn Thompson writes in an MSNBC article of a raid by federal agents on a home that was linked to downloaded child pornography. The identity and location of the subscriber were provided by the ISP. The desktop computer, iPhones, and iPads of the homeowner and his wife were seized in the raid. Federal agents returned the equipment after determining that no one at the home had downloaded the illegal material. Agents eventually traced the downloads to a neighbor who had used multiple IP subscribers' Wi-Fi connections (including a secure connection from the State University of New York). *See* Carolyn Thompson, *Bizarre Pornography Raid Underscores Wi-Fi Privacy Risks* (April 25, 2011), http://www.msnbc.msn.com/id/42740201/ns/technology_and_science-wireless/

given location is the same individual who allegedly downloaded a single sexually explicit film is tenuous, and one that has grown more so over time." *Id.* at *3.

Lastly, Rule 15(c)(3) permits an amended complaint to relate back only where there has been an error made concerning the identity of the proper party and where that party is chargeable with knowledge of the mistake. It does not permit relation back where, as here, there is a lack of knowledge of the proper party to begin with. *Miller v. Mancuso*, 388 Fed. Appx. 389, 391 (5th Cir. 2010); *Wilson v. U.S.*, 23 F.3d 559, 563 (1st Cir. 1994). For these reasons alone, there are serious issues around the credibility of evidence proffered by the Plaintiff in support of its subpoena request.

III. ARGUMENT

A. John Doe 112 Has Standing to Quash.

Doe 112 has standing as a party to this action, though not yet designated as such. Plaintiff seeks to impose joint and several liability upon John Doe *and* his co-conspirators, though at present it asserts only John Doe is a party. However, a nonparty cannot be bound by a case in which he or one in privity with him is not a party unless the party is represented in the action and the representation is full and adequate. *Hansberry v. Lee,* 311 U.S. 32 (1940); *Smith v. Bayer Corp.*, 131 S. Ct. 2368, 2379 (U.S. 2011).

An individual becomes a party when sufficiently identified in the complaint, whether by an actual or fictitious name. The Complaint sufficiently identifies John Doe 112 as a co-conspirator through his "unique IP address" he was assigned at the time of alleged infringement. ECF No. 2-1, ¶ 24 ("Hansmeier Declaration").

> "The court notes that it cannot ignore the inconsistency of the plaintiff's position that the Doe … lacks standing to pursue a motion to [quash] because it has not been named or served, but at the same time refer throughout the … complaint to the [co-conspirator] who the plaintiff expressly identifies in the … complaint as the person with the Internet Protocol address [184.155.204.241]. … For all intents and purposes, the plaintiff has filed a complaint naming Doe [112] IP Address [184.155.204.241] as a [co-conspirator]. The plaintiff's contention otherwise does not make it so."

Millenium TGA, Inc. v. Does 1-800, No. 10-cv-05603, 2011 U.S. Dist. LEXIS 94746, *3-4 (N.D. Ill. Aug. 24, 2011) (*citing, Lake v. Neal*, 585 F.3d 1059 (7th Cir. 2009) ("[I]f it walks like a duck, swims like a duck, and quacks like a duck, it's a duck.").

> "The status of parties, whether formal or otherwise, does not depend upon the names by which they are designated, but upon their relation to the controversy involved, its effect upon their interests, and whether judgment is sought against them. When, as here, the cause of action is against them, and substantial relief sought against them, they are real parties in interest."

Abels v. State Farm Fire & Casualty Co., 770 F.2d 26, 30 n.3 (3rd Cir. Pa. 1985) (*citing, Grosso v. Butte Elec. Ry. Co.*, 217 F. 422, 423 (D. Mont. 1914); *Ramirez v. Michelin N. Am., Inc.*, No. 07-cv-00228, 2007 U.S. Dist. LEXIS 52244, *12 n.8 (S.D. Tex. July 19, 2007).

As the court in *Simmons* observed, a defendant may be designated by a fictitious name, such as "IP address 184.155.204.241", if his true name is unknown to the Plaintiff and the Plaintiff *intends* to substitute the real name of the Defendant once his true name is ascertained. *Simmons v. District of Columbia*, 750 F. Supp. 2d 43, 45 (D.D.C. 2011).

Though expedited discovery was granted on February 9, 2012, Plaintiff "has yet to amend [the] complaint to include John Doe's co-conspirators as defendants in this action"—perhaps because it never intends to. Complaint, ¶ 38. A non-party to an action cannot be subpoenaed to produce documents pursuant to Rule 45(b) if there is no legal proceeding contemplated. *Taylor v. Litton Medical Products, Inc*., 19 Fed. R. Serv. 2d 1190, 1191-92 (D. Mass. 1975) ("that the defendant cannot subpoena documents for the purpose of inspection and investigation with the view to eventually subpoenaing them to a trial or deposition or other legal proceeding").

> "One reason for the restrictive interpretation is the potential for abuse of the subpoena. The subpoena invokes the power of the Court and, therefore, has the capacity to disrupt the lives of [John Doe 112]. A procedure which allowed parties to send out subpoenas *duces tecum* at will could result in a form of one-sided discovery."

Id. See also, Turner v. Parsons, 596 F. Supp. 185, 186 (E.D. Pa. 1984). Indeed, Plaintiff's failure to serve any of the 3,868 defendants it has filed suit against, belies Plaintiff's true intentions.

To prevent John Doe 112 from challenging the subpoena begs the question as to whether the proceedings are truly adversarial or little more than an attempt to use expedited discovery to wrest quick settlements, regardless of innocence. *On the Cheap, LLC v. Does 1-5011*, No. 10-cv-04472, 2011 U.S. Dist. LEXIS 99831 (N.D. Cal. 2011). *See also, VPR Internationale v. Does 1-1017*, No. 11-cv-02068, 2011 U.S. Dist. LEXIS 64656 (C.D. Ill. 2011).

B. This Court Lacks Personal Jurisdiction over Moving Defendants and Dismissal is Appropriate Under Fed. R. Civ. P. 12(b)(2).

The Plaintiff has stated, after discovery of the identity connected to each IP address, it intends "to seek leave of the Court to amend this complaint to join John Doe's co-conspirators as defendants in this action pursuant to Fed. R. Civ. P. 20(a)(2) so long as the Court has jurisdiction over those individuals." Complaint, ¶ 38. At the time it filed its Complaint, Plaintiff already knew which 'co-conspirators' this Court had jurisdiction over and that John Doe 112 was not among them.

> "Plaintiff used geo-location technology to trace the IP address of John Doe to a point of origin within the State of Texas. Geo-location is a method for ascertaining the likely geographic region associated with a given IP address at a given date and time."

Complaint, ¶ 6.

As Plaintiff readily acknowledges, IP addresses serve as a useful tool to determine the general geographic location of the user. For example, a query submitted to http://domaintz.com/tools/reverse-ip/ for the IP address listed on Plaintiff's subpoena for John Doe 112 (184.155.204.241), returns the result as shown in Exhibit A. To verify this information, a user can access another free tool like http://whatismyipaddress.com/, as shown in Exhibit B. In each, entering "184.155.204.241" returns a location of Rio Rancho, New Mexico.

Thus, without any of the information sought in the subpoena, the Plaintiff already knows that the John Doe 112 is a resident of New Mexico and not subject to this Court's jurisdiction. Consequently, the Court may not authorize or enforce any discovery Plaintiff seeks about John Doe 112. *Cent. States, Se. & Sw. Areas Pension Fund v. Phencorp Reinsurance Co., Inc.*, 440 F.3d 870, 877 (7th Cir. 2006) (holding that a prima facie case for personal jurisdiction must be made before discovery is allowed); *see also Enterprise Int'l v. Corporacion Estatal Petrolera Ecuatoriana*, 762 F.2d 464, 470-471 (5th Cir. 1985) (no authority to issue preliminary relief without personal jurisdiction); *accord United Elec. Radio and Mach. Workers of America v. 163 Pleasant Street Corp.*, 960 F.2d 1080, 1084 (1st Cir. 1992) (same). Therefore, and contrary to the Plaintiff's suggestion, the jurisdictional question is a live issue that the Court can and should consider before allowing this action to move any further.

C. Plaintiff's Request for Discovery Disregards John Doe 41's Privacy Rights.

The Plaintiff is not seeking information about John Doe 112's IP address for the purpose of litigating its current claims against John Doe, the Defendant. Instead, the Plaintiff purportedly intends to sue John Doe 112 in a separate action at a later date using the information it discovers now.[13]

When evaluating relevancy, "a court is not required to blind itself to the purpose for which a party seeks information." *Oppenheimer Fund, Inc. v. Sanders,* 437 U.S. 340, 353 (1978). Thus, "when the purpose of a discovery request is to gather information for use in proceedings other than the pending suit, discovery properly is denied." *Id.* That is precisely the situation here.

Plaintiff contends that Internet subscribers like John Doe 112 do not have an expectation of privacy in their subscriber information "because they have already conveyed such information to their Internet Service Providers." Memorandum, ECF No. 2, p.9.

If John Doe 112 truly has no privacy interest in his information being disclosed, then this Court need not have granted the subpoena in the first place. The Plaintiff could have just called John Doe 112's ISP and simply obtained the subscriber information without any resistance.

> "Whatever privacy interest that a customer may have in the contact information associated with an IP address is minimal at best. … Still, however minimal or 'exceedingly small' the … interests here are, parties need only have 'some personal right or privilege in the information sought' to have standing to challenge a subpoena to a third party. *Robertson v. Cartinhour*, 2010 U.S. Dist. LEXIS 16058, 2010 WL 716221, *1 (D. Md. Feb. 23, 2010). Accordingly, it appears that the Doe Defendants have standing to contest the subpoenas, and their motions to quash will not be denied on that basis."

Third Degree Films, Inc. v. Does 1-108, No. 11-cv-03007, 2012 U.S. Dist. LEXIS 25400, *7-8 (D. Md. Feb. 28, 2012).

> "Just as police cannot invade the privacy of a home without some concrete evidence of wrongdoing inside, plaintiffs should not be able to use the Court to invade others' anonymity on mere allegation. By requiring plaintiffs to make out a prima facie case of infringement, the standard requires plaintiffs to adduce evidence showing that their complaint and subpoena are more than a mere fishing expedition."

London-Sire Records, Inc. v. Doe 1, 542 F. Supp. 2d 153, 175 (D. Mass. 2008).

Other courts recognize an allegation that an individual illegally downloaded adult entertainment goes to matters of a sensitive and highly personal nature, including one's sexuality.

---

[13] More likely, the Plaintiff will use the information to coerce a settlement.

United States ex rel. Doe v. Boston Scientific Corp., 2009 U.S. Dist. LEXIS 59390, *9-10 (S.D. Tex. July 2, 2009) (citing *Does I Thru XXIII v. Advanced Textile Corp.*, 214 F.3d 1058, 1068 (9th Cir. 2000). The privacy interests of innocent third parties as well as the nature of the accusation, weighs heavily against the Plaintiff's access to the requested information absent a showing that the John Doe 112 is the actual infringer. *Third Degree Films v. Does 1-3577*, No. 11-cv-02768, 2011 U.S. Dist. LEXIS 128030, *11 (N.D. Cal. Nov. 4, 2011) (*citing, Gardner v. Newsday, Inc.*, 895 F. 2d 74, 79-80 (2d Cir. 1990)).

D. Subpoenas Seek Non-Relevant Information.

A plaintiff seeking to identify anonymous defendants "must demonstrate that the specific information sought by subpoena is necessary to identify the defendant and that the defendant's identity is relevant to the plaintiff's case." *Salehoo Grp., Ltd. v. ABC Co.*, 722 F. Supp. 2d 1210, 1216 (W.D. Wash. 2010).

The identity of John Doe 112 connection with a non-party IP address is not relevant to the pending claims against the Defendant, John Doe. Discovery is appropriate only if the information sought is relevant, which means that it is "reasonably calculated to lead to the discovery of admissible evidence." Fed. R. Civ. P. 26(b)(1); *see also, Williams v. Blagojevich*, No. 05-cv-04673, 2008 U.S. Dist. LEXIS 643, *3 (N.D. Ill. Jan. 2, 2008) ("The scope of material obtainable by a Rule 45 subpoena is as broad as permitted under the discovery rules.") (citations omitted).

Where no proceedings beyond the *ex parte* motion are envisioned by Plaintiff, the information is not necessary or relevant to the case, because there is no case. A nonparty cannot be subpoenaed to produce documents pursuant to Rule 45(b) if there is no legal proceeding contemplated. *Taylor v. Litton Medical Products, Inc.*, 19 Fed. R. Serv. 2d 1190, 1191-92 (D. Mass. 1975).

> [A] subpoena duces tecum is limited to use in conjunction with a deposition and trial. One reason for the restrictive interpretation is the potential for abuse of the subpoena. ... A procedure which allowed parties to send out subpoenas *duces tecum* at will could result in a form of one-sided discovery.

Bowers v. Buchanan, 110 F.R.D. 405, 406 (S.D. W. Va. 1985) (citing cases); see also *Theofel v. Farley-Jones*, 359 F. 3d 1066, 1074 (9th Cir. 2004) ("The subpoena power is a substantial delegation of authority to private parties, and those who invoke it have a grave responsibility to ensure it is not abused."). To justify a Rule 45 subpoena Plaintiff must have a

"genuine intent to take" discovery for use in conjunction with deposition and trial. *Greenberg v. United States*, Civ. A. No. 89-2390-MC, 1990 U.S. Dist. LEXIS 12091, *5 (D. Mass. Sept. 7, 1990) (citing, inter alia, *Bowers*); see also *London-Sire Records v. Doe 1*, 542 F. Supp. 2d 153, 164 (D. Mass. 2008) (requiring showing of "a central need for the subpoenaed information to advance the claim"). Without any genuine defendants, there is no basis for discovery. *Bessette v. Avco Fin. Servs., Inc.*, 279 B.R. 442, 454 (D.R.I. 2002) ("This Court cannot sanction the further progression of an adversarial proceeding where there is no opposing party."); *Tillson v. Odyssey Cruises*, No. 8-cv-10997-DPW, 2011 U.S. Dist. LEXIS 7911, *1 n.1 (D. Mass. Jan. 27, 2011) (dismissing claims against unidentified Doe defendants).

The Plaintiff attempts to justify the scope of the subpoenas in this single John Doe defendant case by alleging the existence of additional IP addresses representing "co-conspirators" who conspired to infringe the Plaintiff's copyright by downloading the same film through BitTorrent. The Plaintiff's contention, in essence, is that the identity of a non-party, whom the Court does not have jurisdiction over, associated with the IP address, who may or may not be sued, will be relevant to pursuing claims in the present litigation against John Doe.

By this device, the Plaintiff can avoid all personal jurisdiction and joinder hurdles, and yet obtain the identifying information connected with hundreds of IP addresses located all over the country through a single lawsuit. Of course, bringing suit against the co-conspirators, may not be necessary, because the Plaintiff can use the identifying information to leverage a settlement before ever suing. *See, Digiprotect USA Corp. v. Does 1-266*, No. 10-cv-08759, 2011 U.S. Dist. LEXIS 40679, *2 (S.D.N.Y. Apr. 13, 2011) ("The court…remains concerned[] that defendants over whom the court has no personal jurisdiction will simply settle with plaintiff rather [than] undertake the time and expense required to assert their rights.").

To have relevance to the pending action, the requested discovery must bear on the civil conspiracy and copyright claims against the current John Doe defendant. In light of the structure of BitTorrent, subpoenas seeking the identity of subscribers of non-party IP addresses are not reasonably calculated to lead to the discovery of evidence relevant to the pending claims. BitTorrent users remain anonymous to other BitTorrent users, and have no connection to them beyond the mere fact that they downloaded the same file. It is true that, assuming the BitTorrent users were accessing the network at the same time, they may have downloaded and uploaded

pieces of the same file from each other's computers as part of the same swarm. *See, MCGIP, LLC v. Does 1-30*, No. 11-cv-03680, 2011 U.S. Dist. LEXIS 88790, *1 (N.D. Cal. Aug. 10, 2011). Nonetheless, a BitTorrent user need not communicate with other users in any other way. *Id.* Indeed, a BitTorrent user will have no information about other users other than their IP addresses —the same information the Plaintiff already possesses. *Id.*; *cf. Hard Drive Prods., Inc. v. Does 1-188,* 809 F. Supp. 2d 1150, 1163 (N.D. Cal. 2011) ("[E]ven if the IP addresses at issue … all came from a single swarm, there is no evidence to suggest that each of the addresses 'acted in concert' with all of the others."). It is therefore not a reasonable calculation that the individual connected to the subpoenaed IP address will have any discoverable information related to the current Defendant.

E. Plaintiff Fails to Adequately State a Claim for Civil Conspiracy.

To succeed in a claim of civil conspiracy under Texas law, the Plaintiff must establish an agreement between two or more persons for the purpose of accomplishing either an unlawful purpose or a lawful purpose by unlawful means and at least one tortious act by one of the co-conspirators in furtherance of the agreement that caused an injury to the plaintiff. *Robinson v. Castle,* 2011 U.S. Dist. LEXIS 96861,*27 (S.D. Tex. Aug. 29, 2011) (*citing, Massey v. Armco Steel Co*., 652 S.W.2d 932, 934 (Tex. 1983)).

As pled, the existence of a conspiracy is simply not plausible, because 1) the Plaintiff has not pled, nor can it, the existence of an agreement among the Defendant and John Doe 112 or any of the 938 alleged conspirators; and 2) the Plaintiff has failed to allege the Defendant or co-conspirators downloaded *the same file*. Complaint, ¶ ¶ 33-37. An agreement is a necessary and important element of this cause of action. *Robinson* at *27.

Plaintiff alleges that, by virtue of BitTorrent, "[t]he [Defendant and his co-conspirators] were collectively engaged in the conspiracy even if they were not engaged in the swarm contemporaneously because they all took concerted action that contributed to the chain of data distribution." Complaint, ¶ 33. But under Plaintiff's logic, all persons within a single swarm—even if that swarm continues for months on end and contained hundreds or thousands of BitTorrent users—would be appropriately joined as co-conspirators in a single copyright infringement action. In addressing the plaintiff's civil conspiracy claim, the *Pacific Century International* court found that:

> [a]lthough [p]laintiff explains the protocol and how it differs from its predecessor P2P programs, and specifically claims that [d]efendants have engaged in a civil conspiracy … [p]laintiff still has failed to demonstrate that it has 'any right to relief against [Defendants] … arising out of the same transaction, occurrence, or series of transactions or occurrences.

Pacific Century International Ltd. v. Does 1-101, No. 11-cv-02533, 2011 U.S. Dist. LEXIS 73837, *4 (N.D. Cal. July 8, 2011) (citing Fed.R.Civ.P. 20(a)(2)(A)).

The declaration submitted in this action, like the declaration in *Boy Racer*, contradicts the assertion that the Does in this action are part of a single swarm. *Boy Racer v. Does 2-52,* No. 11-cv-02834, ECF No. 3-1 (N.D. Cal. June 14, 2011), attached as Exhibit B. Though the *Hansmeier Declaration* argues at length about the "concerted activity" within a given swarm to support Plaintiff's conspiracy claim, the affiant refers to *multiple* swarms throughout his declaration. Users in different swarms have nothing in common other than downloading the same work, which as this court and others have noted is insufficient under our precedent. *See,* Hansmeier Decl., ¶ 13 ("[the first step in the infringer-identification process is to locate swarms where peers are distributing the copyrighted creative works."); ¶ 14 ("I used all three methods to locate swarms associated with Plaintiff's exclusive license."). Several courts have noted this identical problem. *See, e.g., Hard Drive Productions, Inc. v. Does 1-188,* No. 11-cv-01566, 2011 U.S. Dist. LEXIS 94319, *14 (N.D. Cal. Aug. 23, 2011); *Boy Racer v. Does 2-52,* No. 11-cv-02834, 2011 U.S. Dist. LEXIS 86746, *8 (N.D. Cal. Aug. 5, 2011) ("But the Hansmeier declaration itself offers overwhelming evidence that the IP addresses were in fact gathered from multiple swarms.").

A swarm is defined by a hash number. The hash is a string of alphanumeric characters (typically hexadecimal) in the .torrent file that the client uses to verify the data that is being transferred. When a user chooses to download a torrent from a list, the .torrent file is automatically searched for by hash value. That is, each piece of the overall file must share the same hash number for the pieces to be assembled together into the completed file/film. Thus, a single film may be the subject to multiple swarms, with each swarm constituting a distinct and separate infringement.

For a conspiracy to be proper the Plaintiff must show that the alleged conspirators agreed to all share the same *file*, not the same film. Conspiracy based on separate but similar acts of copyright infringement over the Internet has not only been rejected repeatedly by courts across the country. Indeed, the Does here are not even alleged to have infringed the same movie. *See,* First

Amended Complaint, Ex. A (providing no hash values for alleged infringements). This kind of attenuated relationship is not sufficient for conspiracy.

Even if the IP addresses at issue all came from a single swarm, Plaintiff has failed to show that any of the co-conspirators "acted in concert" or actually exchanged any piece of the seed file with one another.

> "In this age of instant digital gratification, it is difficult to imagine, let alone believe, that an alleged infringer of the copyrighted work would patiently wait six weeks to collect the bits of the work necessary to watch the work as a whole. At the very least, there is no proof that bits from each of these addresses were ever assembled into a single swarm. As the court previously explained, under this court's precedent regarding other file sharing protocols, merely infringing the same copyrighted work over this period is not enough."

See, Boy Racer, Inc. v. Does 1-60, No. 11-cv-01738 SI, 2011 U.S. Dist. LEXIS 92994, *4 (N.D. Cal. Aug. 19, 2011).

Plaintiff's complaint attempts to address this issue by alleging that "[t]he Defendants were collectively engaged in the conspiracy even if they were not engaged in the swarm contemporaneously because they all took concerted action that contributed to the chain of data distribution." Complaint, ¶ 33. Here, the alleged "chain of data distribution" spans 939 conspirators, allegedly infringing at 939 different times, and over a two-month period between October 10, 2011 and December 5, 2011. *See,* Complaint, Ex. A. Absent evidence that the Doe defendants actually acted in concert to illegally download the same file on those 36 separate days (and Plaintiff provides none), a conspiracy claim is inappropriate. *See, e.g., Boy Racer,* No. 11-cv-01738, 2011 U.S. Dist. LEXIS 92994, *4; *Hard Drive Productions, Inc. v. Does 1-188,* No. 11-cv-01566, 2011 U.S. Dist. LEXIS 94319, *7-14 (N.D. Cal. Aug. 23, 2011) (collecting cases); *AF Holdings LLC v. Does 1-97,* No. 11-cv-03067, 2011 U.S. Dist. LEXIS 78636, *4 (N.D. Cal. July 20, 2011) (holding that even though BitTorrent differ from previous peer-to-peer platforms, joinder is improper)

As other courts have noted, Plaintiff's Complaint and Mr. Hansmeier's declaration are templates that not tailored to the facts of this case. Mr. Hansmeier makes no reference to "Shemale Yum—Jenna Comes A' Knocking!," "so it is unclear whether Mr. Hansmeier, himself, understands which copyrighted work is at issue in this action." *OpenMind Solutions, Inc. v. Does 1-39,* No. 11-cv-03311, 2011 U.S. Dist. LEXIS 94356, *2 (N.D. Cal. Aug. 23, 2011).

V. CONCLUSION

Plaintiff has the right to seek legal redress for alleged copyright infringement, but it must follow the basic procedures and due process requirements applicable to all civil litigation. Denying discovery about John Doe's IP address will not leave the Plaintiff without a remedy to uncover his identity or those of the other purported copyright infringers. The Plaintiff need merely sue each IP address in the district in which the address is located, and then subpoena the ISPs for identifying information pertaining to that IP address. What the Plaintiff may not do, however, is improperly use court processes[14] by attempting to gain information about hundreds of IP addresses located all over the country in a single action, especially when many of those addresses knowingly fall outside of the court's jurisdiction. Moving Defendant therefore respectfully urges this Court to vacate its ruling on Plaintiff's Motion for Expedited Discovery, quash the subpoena already issued by the Plaintiff, and drop the John Doe 112 from this action.

Dated: June 29, 2012

Respectfully,

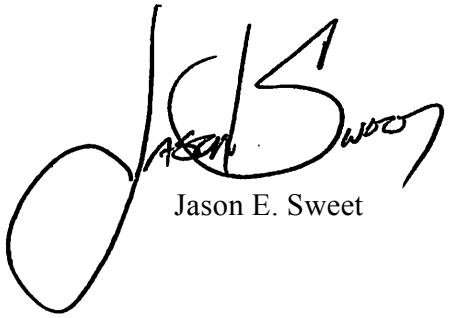
Jason E. Sweet (BBO# 668596)
BOOTH SWEET LLP
32R Essex Street
Cambridge, MA 02139
Tel.: (617) 250-8619
Fax: (617) 250-8883
Email: jsweet@boothsweet.com

Pro Hac Vice Appearance

[14] In addition to the procedural improprieties outlined above, the Plaintiff's tactics deny the federal courts additional revenue from filing fees in the suits that should be filed to obtain the information the plaintiffs desire. *CP Productions, Inc. v. Does 1-300,* No. 10-cv-6255, 2011 U.S. Dist. LEXIS 113013, *1 ("No predicate has been shown for thus combining 300 separate actions on the cheap—if CP had sued the 300 claimed infringers separately for their discrete infringements, the filing fees alone would have aggregated $105,000 rather than $350.").

CERTIFICATE OF SERVICE

I hereby certify that on June 29, 2012, the foregoing document, filed through the ECF system, will be sent electronically to the registered participants as identified on the Notice of Electronic Filing, and paper copies will be served via first-class mail to those indicated as non-registered participants.



Jason E. Sweet